

# Assessing the Security of Federal Information Technology Systems

*The Development of Standardized Certification and Accreditation Guidelines and Provider Organizations*

Dr. Ron Ross

# Today's Climate

- Highly interactive environment of powerful computing devices and interconnected systems of systems across global networks
- Federal agencies routinely interact with industry, private citizens, state and local governments, and the governments of other nations
- The complexity of today's systems and networks presents great security challenges for both producers and consumers of information technology

# Today's Challenge

- Need for greater confidence in the security of enterprise IT systems
- Need for consistency in the approaches used to assess the capabilities and limitations of IT systems in Federal agencies

skill sets to conduct IT system assessments

## *Building more secure systems requires --*

- Well defined system-level security requirements and security specifications
- Well designed component products
- Sound systems security engineering practices
- Competent systems security engineers
- Appropriate metrics for product/system testing, evaluation, and assessment
- Comprehensive system security planning and life cycle management

# The Security Chain



## Links in the Chain

(Non-technology based examples)

- ✓ Physical security
- ✓ Personnel security
- ✓ Procedural security
- ✓ Risk management
- ✓ Security policies
- ✓ Security planning
- ✓ Contingency planning

## Links in the Chain

(Technology based examples)

- ✓ Access control mechanisms
- ✓ Identification and authentication devices
- ✓ Audit mechanisms
- ✓ Encryption mechanisms
- ✓ Firewalls
- ✓ Smart cards
- ✓ Biometrics

Adversaries attack the weakest link...where is yours?

# National Policy

Office of Management and Budget Circular A-130,  
*Management of Federal Information Resources*  
requires federal agencies to:

- Plan for security
- Ensure that appropriate officials are assigned security responsibility
- Authorize system processing prior to operations and periodically, thereafter.

# Achieving Adequate Security

- OMB Circular A-130 defines *adequate security* as security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information
- Adequate security emphasizes the risk-based policy for cost-effective security established by Public Law 100-235, the Computer Security Act of 1987

# System Accreditation

*“A management decision by a senior agency official to authorize operation of an IT system based on the results of a certification process and other relevant considerations...”*

- Assigns responsibility for the safe and secure operation of an IT system to a designated authority
- Balances mission requirements and the residual risks to an IT system after the employment of appropriate protection measures (security controls)



# Security Certification

*“**A** comprehensive analysis of the technical and non-technical aspects of an IT system in its operational environment to determine compliance to stated security requirements and controls...”*

- Employs a set of structured verification techniques and verification procedures during the system life cycle
- Demonstrates the security controls for an IT system are implemented correctly and are effective
- Identifies risks to confidentiality, integrity, and availability of information and resources

# Program Objectives

## *Phase I*

- To develop standardized guidelines for conducting security certifications and accreditations of federal IT systems

## *Phase II*

- To create a national network of accredited organizations capable of providing cost effective, quality security assessment services based on the standardized guidelines

*PHASE I*

# Development of Guidance

- NIST Special Publication 800-37  
*Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems*
- NIST Special Publication 800-53  
*Minimum Security Controls for Federal Information Technology Systems*
- NIST Special Publication 800-53A  
*Techniques and Procedures for the Verification of Security Controls in Federal Information Technology Systems*

## *PHASE II*

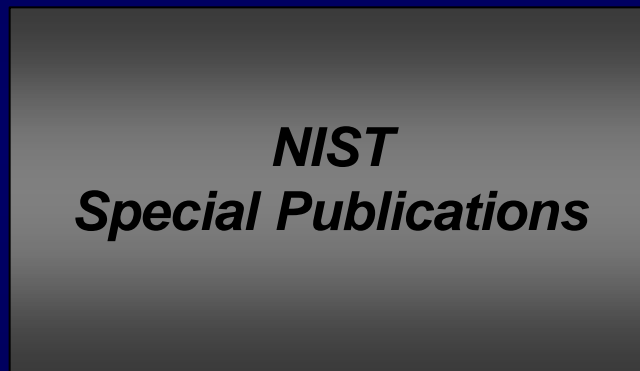
# Development of Capability

- Create criteria for accrediting public and private sector organizations to conduct security certifications in accordance with NIST Special Publications 800-37, 800-53, 800-53A
- Develop associated proficiency tests to demonstrate assessment organization competence
- Accredite public and private sector enterprises to conduct security certifications by Fall 2004

# Development Strategy

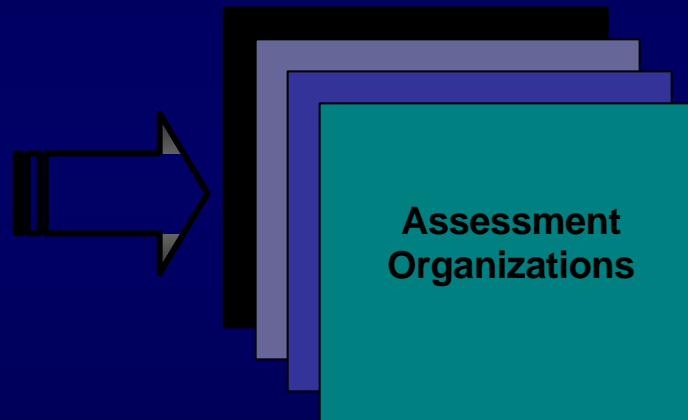
- Limited federal government involvement
  - **Develop and maintain standardized system certification and accreditation guidelines (Special Publication 800-37)**
  - **Develop and maintain standardized (minimum) security controls and verification techniques/procedures (Special Publications 800-53 and 800-53A)**
  - **Develop and maintain assessment organization program (i.e., accreditation criteria and assessment methods for participating organizations)**
  - **Accredit public and private sector assessment organizations to for competence**
- Maximum use of private sector capabilities
  - **Collaborate with industry on security C&A guideline development**
  - **Encourage private sector development of C&A tools and training classes**
  - **Use private sector assessment organizations to conduct security certifications for federal customers (when desired)**

## Standardized Guidelines for Certification and Accreditation



*A flexible, tailorable, and robust security certification process for federal agencies*

## Network of Accredited Assessment Organizations



### **Non-Technical Issues**

- ✓ Physical Security
- ✓ Personnel Security
- ✓ Procedural Security
- ✓ Administrative Security

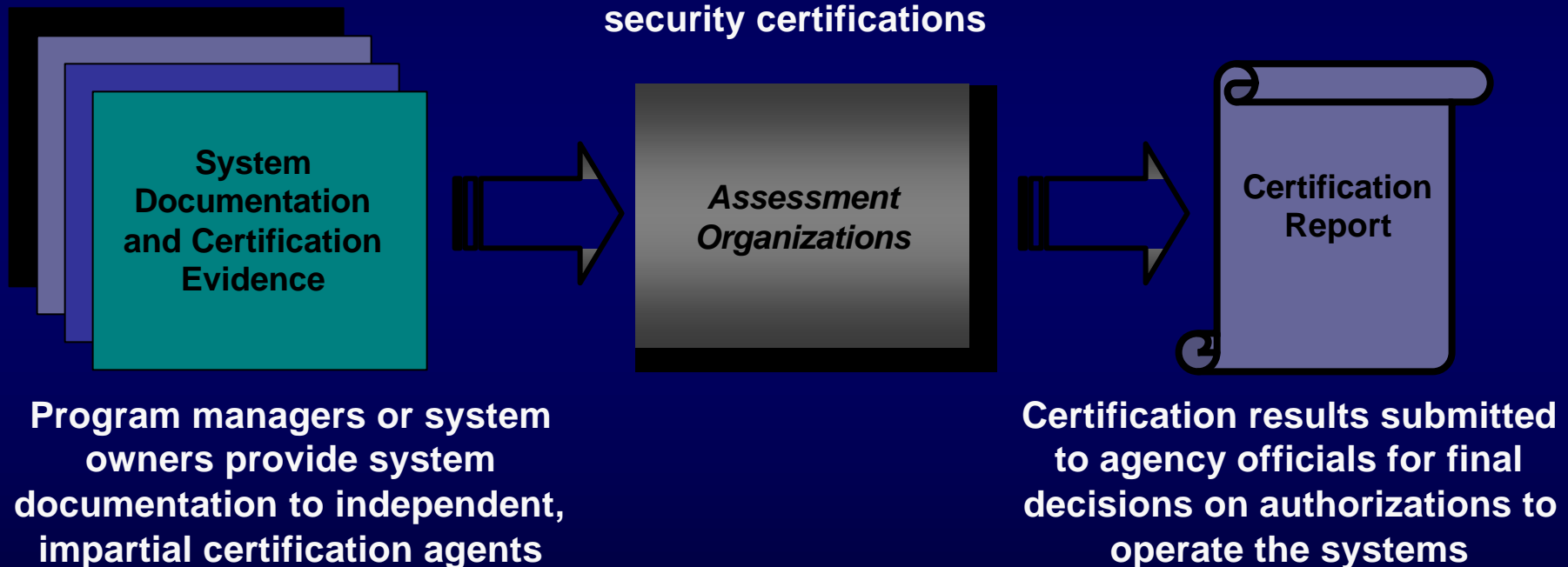
### **Technical Issues**

- ✓ Access Control
- ✓ Identification
- ✓ Authentication
- ✓ Auditing
- ✓ Communications

*Competent providers of security assessment services*

# Assessing System Security

Public and private sector, accredited  
assessment organizations conduct  
security certifications



# Significant Features

- Employs a standardized process for the certification and accreditation of IT systems
- Integrates the use of standardized security controls and standardized verification techniques/procedures
- Minimizes documentation required and produced during the C&A process
- Maximizes the cost-effective production of essential evidence to support informed, risk-based accreditation decisions by senior agency officials



# Significant Benefits

- More consistent, comparable, and repeatable system-level evaluations or system certifications of federal IT systems
- More complete, reliable technical information for IT system accreditation authorities—leading to better understanding of complex systems and associated risks and vulnerabilities
- Greater availability of competent certification services for public and private sector customers

# Special Publication 800-37

## *Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems*

- Establishes a standard process, general tasks and specific subtasks to certify and accredit IT systems supporting the executive branch of the federal government
- Focuses on federal systems processing, storing and transmitting sensitive (unclassified) information but can be applied to national security or intelligence systems, if so directed by appropriate authorities
- Supercedes NIST Federal Information Processing Standards (FIPS) Publication 102

Note: Projected publication Fall 2002.

# Special Publication 800-53

1

## *Minimum Security Controls for Federal Information Technology Systems*

- Provides standardized security controls for confidentiality, integrity, and availability
- Arrays controls in a standard package of basic controls (low levels of concern for C, I, A)
- Offers optional controls for moderate and high levels of concern in agency-defined supplemental package
- Integrates security controls from many sources—policies, directives, and guidelines (e.g., NIST SP 800-26, DoD 8500, D/CID 6-3, ISO/IEC 17799, and GAO FISCAM)

Note: Projected publication Spring 2003.

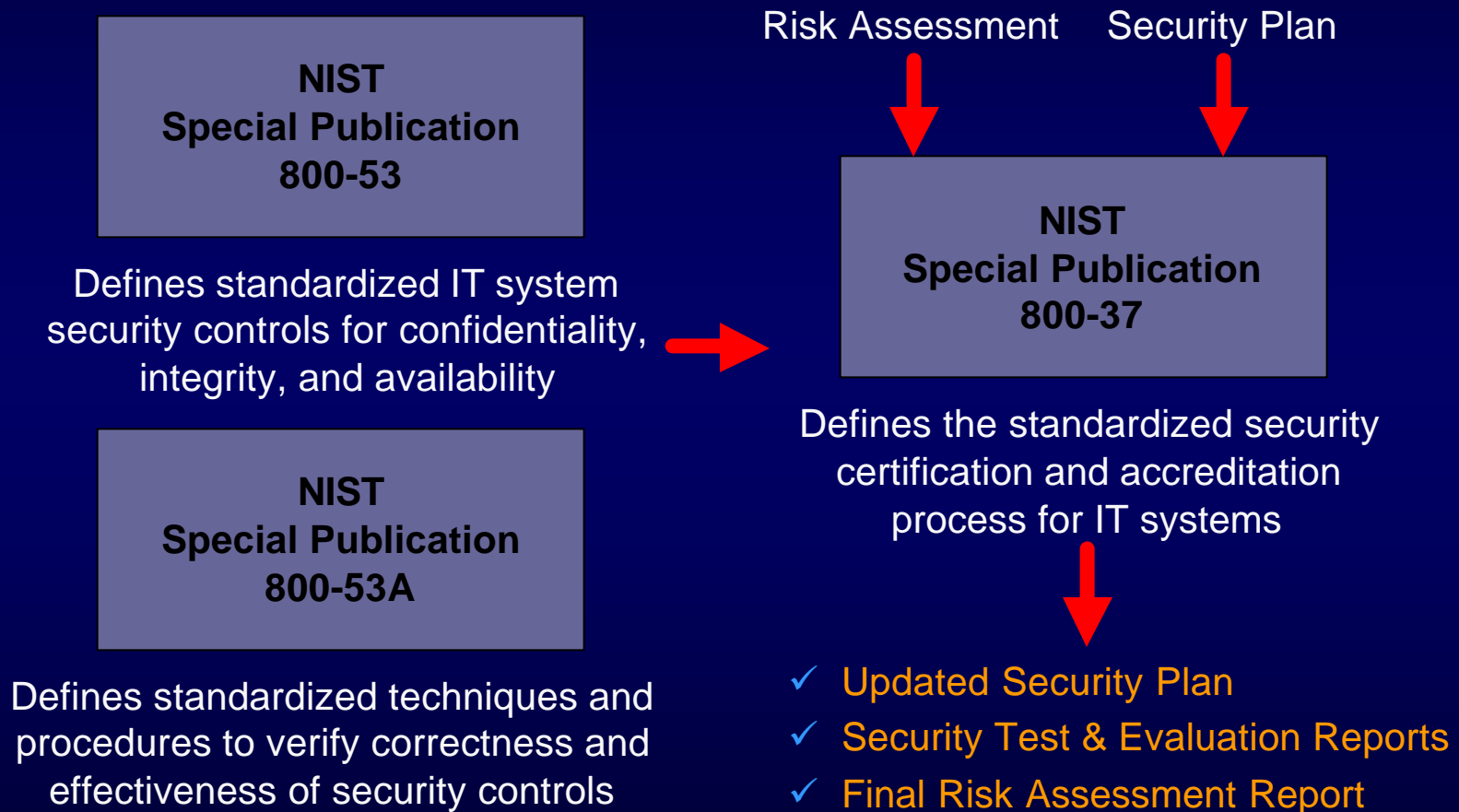
# Special Publication 800-53A

## *Techniques and Procedures for the Verification of Security Controls in Federal Information Technology Systems*

- Provides standardized verification techniques and detailed verification procedures for security controls in SP 800-53
- Associates verification techniques with the Security Certification Levels in SP 800-37 and addresses the level of rigor applied to the security test and evaluation activities
- Specifies certifier actions necessary to demonstrate correct and effective implementation of security controls in SP 800-53

Note: Projected publication Spring 2003.

# Security Accreditation Model



# Phases of the C&A Process

- Pre-certification Phase
- Certification Phase
- Accreditation Phase
- Post-accreditation Phase

# Key Security Factors

- Confidentiality

- Assurance that information in an IT system is not disclosed to unauthorized persons, processes or devices

- Integrity

- Assurance that information in an IT system is protected from unauthorized, unanticipated, or unintentional modification or destruction

- Availability

- Assurance that information, services, and IT system resources are accessible to authorized users and/or system-related processes on a timely and reliable basis and are protected from denial of service

# Characterizing an IT System

- Examine the *criticality/sensitivity* of the system and the information the system processes, stores, and transmits
- Assess the *exposure* of the system and its information to both internal and external threats
- Assign appropriate *levels of concern* for both system criticality/sensitivity and exposure



# System Critical/Sensitivity

- The importance and nature of the information processed, stored, and transmitted by the IT system to the organization's mission and day-to-day operations
- Measured by analyzing the system requirements for confidentiality, integrity, and availability

# System Exposure

A measure of the potential risk to an IT system from both external and internal threats:

- *External system exposure factors:*
  - Method by which users access the system, (e.g., dedicated connection, intranet connection, Internet connection, wireless network, PTS connection)
  - Existence of backend connections to the system and to what the backend systems are connected
  - Number of users that access the system
- *Internal system exposure factors:*
  - Security background assurances and/or clearance levels, access approvals, and need-to-know for individuals using the system

# Levels of Concern

(Low, Moderate, High)

- Level of concern for *confidentiality*
  - Based on the tolerance for unauthorized disclosure or compromise of information on the system
- Level of concern for *integrity*
  - Based on the tolerance for unauthorized modification or destruction of information on the system
- Level of concern for *availability*
  - Based on the tolerance for delay in the processing, transmission, or storage of information on the system or the tolerance for the disruption or denial of a service provided by the system

# Levels of Concern

(Low, Moderate, High)

- Level of concern for external exposure
  - Based on the definitions in SP 800-37 (user access methods, backend connections, number of users)
- Level of concern for internal exposure
  - Based on the definitions in SP 800-37 (security background assurances/clearances, access approvals, need-to-know)
- Level of concern for total system exposure
  - Based on the values assigned to both external and internal exposure factors as defined in SP 800-37

# System Characterization

Levels of concern for confidentiality, integrity, availability and system exposure determine:

- Security controls for the IT system
- Security certification level

# Security Certification Level 1

- Independent assessment of an IT system requiring minimal expenditure of resources
- Appropriate for systems engendering:
  - Low levels of concern for confidentiality, integrity, and availability, or
  - Moderate to high levels of concern for confidentiality, integrity, and/or availability *and* systems operating in low to moderate risk environments
- Demonstrates at relatively low levels of assurance that the security controls for an IT system are correctly implemented and are effective in their application
- Employs simple, checklist-based, verification techniques such as personnel interviews, documentation reviews, and observations

# Security Certification Level 2

- Independent assessment of an IT system requiring limited to moderate expenditure of resources
- Appropriate for systems engendering:
  - Moderate levels of concern for confidentiality, integrity, and/or availability, or
  - High levels of concern for confidentiality, integrity, and/or availability *and* systems operating in low to moderate risk environments
- Demonstrates at moderate levels of assurance that the security controls for an IT system are correctly implemented and are effective in their application
- Employs standard, commercially available, assessment tools and verification techniques

# Security Certification Level 3

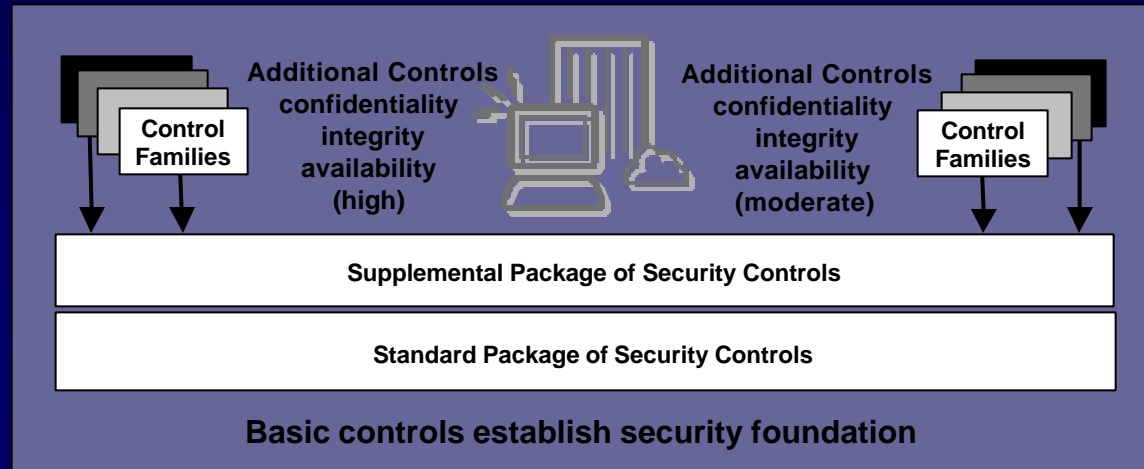
- Independent assessment of an IT system requiring substantial expenditure of resources
- Appropriate for systems engendering high levels of concern for confidentiality, integrity, and availability
- Demonstrates at high levels of assurance, that the security controls for IT systems are correctly implemented and are effective in their application
- Employs the most advanced assessment tools and verification techniques available



# Security Controls

- Management Controls
  - Controls that address the security management aspects of the IT system and the management of risk for the system
- Operational Controls
  - Controls that address the security mechanisms primarily implemented and executed by people (as opposed to systems)
- Technical Controls
  - Controls that address security mechanisms contained in and executed by the computer system

# Customer-Driven Selection



- Baseline of security controls for all IT systems from standard package
- Additional security controls in supplemental package based on increased levels of concern for confidentiality, integrity, and/or availability
- Waivers and/or substitutions of security controls based on system exposure and risk-based decisions

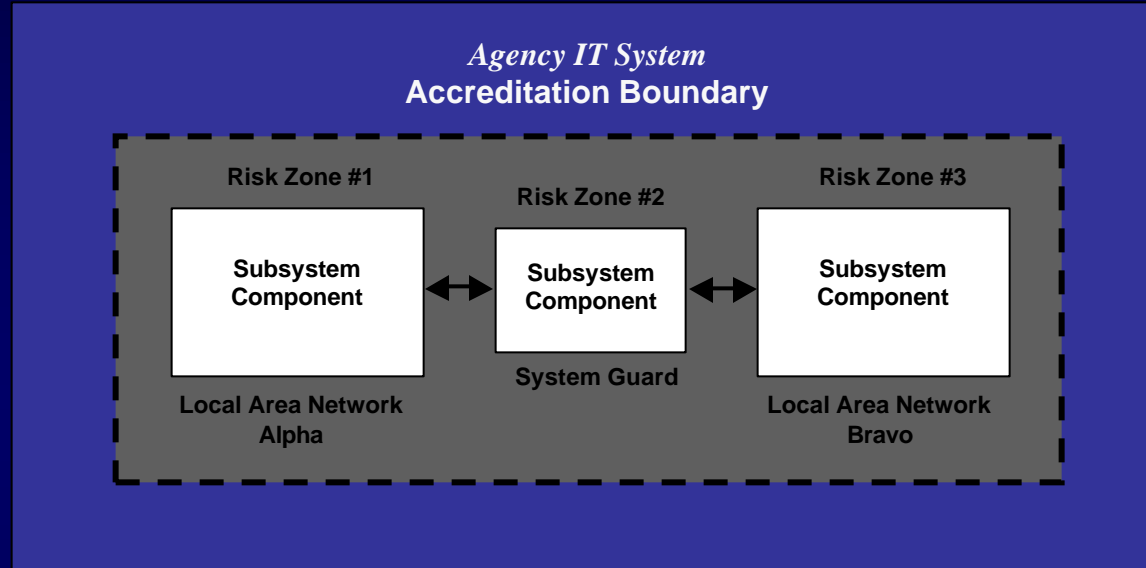
# Large and Complex Systems

- Establish the accreditation boundary for the IT system
- Define a set of system-level components, or subsystems, for both major applications and general support systems
- Subsystem decomposition facilitates the application of the C&A process in a more cost effective manner and supports the concepts of risk management and defense-in-depth
- Each subsystem component is fully characterized in the security plan and an appropriate set of security requirements and security controls identified for that component

# Large and Complex Systems

- Each subsystem component may be certified at a different certification level, depending on the levels of concern expressed by the agency
- The critical, high value subsystem components demand and receive more attention during the certification process than the less important, low-value subsystem components
- The final system accreditation may contain one or more subsystem components certified to the appropriate level based on the documented levels of concern and associated security controls

# Large and Complex Systems



- Security plan reflects the decomposition of the IT system into subsystems
- Each subsystem component is certified at the appropriate certification level
- Risk assessment applied to entire IT system
- Total risk to the system may be greater than the sum of the risks to the individual subsystem components

# Certification Package

## Key Documents---

- Security Plan
- Security Test & Evaluation Reports
- Final Risk Assessment Report
- Certifier's Statement

# Security Plan

- Provides an overview of the security requirements for the IT system
  - Describes the existing or planned security controls (management, operational, and technical) for meeting those requirements
  - Delineates responsibilities and expected behavior of individuals who access the system
- 
- The security plan is a living document that is updated throughout the system development life cycle as new information becomes available.
  - Reference NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998.

# ST&E Reports

- Documents the results of the ST&E activities (verification techniques and verification procedures used to demonstrate the security controls identified in the security plan are correctly implemented and effective)
- Developmental ST&E Report:
  - Applicable to new systems or systems undergoing major upgrades
  - Documents ST&E activities during the development and acquisition phase of the system development life cycle
- Operational ST&E Report:
  - Applicable to new, upgraded, or legacy systems
  - Documents ST&E activities during the implementation or operation/maintenance phases of the system development life cycle



# Final Risk Assessment Report

- Documents threats to and vulnerabilities in the IT system
  - Contains proposals for and evaluations of the effectiveness of various security controls
  - Provides trade-offs associated with the security controls (e.g., performance impact and cost)
  - States residual risk associated with a candidate set of security controls
- The risk assessment report is a living document that is updated throughout the system development life cycle as new information becomes available.
  - Reference NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, January 2002.

# Certifier's Statement

- Provides an overview of the security status of the system and brings together, all of the information necessary for the DAA to make an informed, risk-based decision
- Documents that the security controls are correctly implemented and effective in their application
- Documents the security controls not fully implemented or implemented incorrectly and provides corrective actions

# Accreditation Decisions

- Full Accreditation
- Interim Accreditation
- Accreditation Disapproval

# Accreditation Package

- Conveys DAA's final accreditation decision
  - Constructed from information provided in the certification package
  - Normally consists of:
    - Accreditation letter
    - Security plan
    - Report documenting the basis for the accreditation decision
- Certain information from the security plan, ST&E reports, and risk assessment report may, at the discretion of the DAA, be withheld in the final accreditation package due to its sensitive nature.

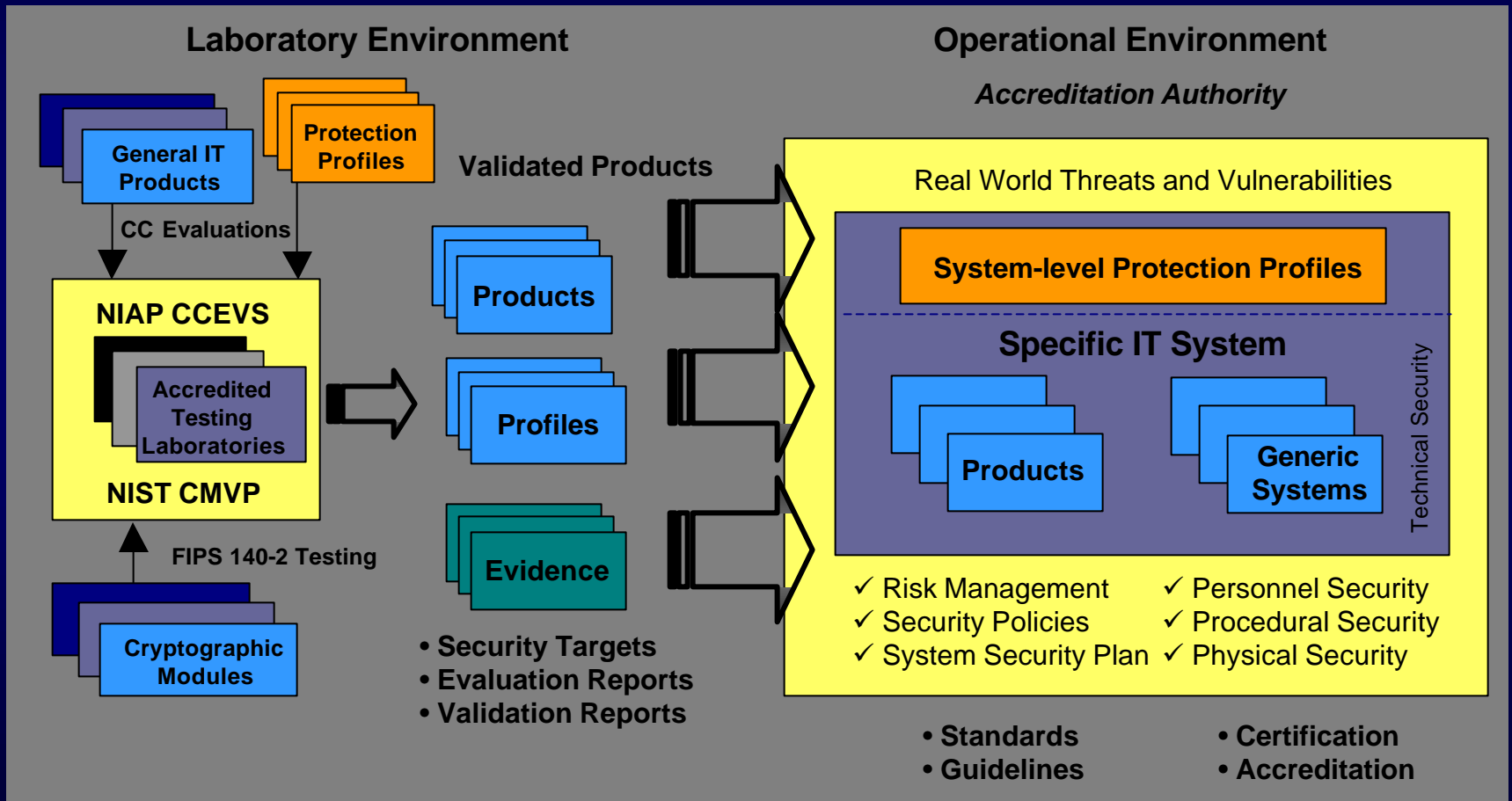
# Product Testing Programs

## Supporting the C&A Process

- NIST Cryptographic Module Validation Program
  - Testing commercial cryptographic modules against U.S. Government Standard (FIPS 140-2 *Security Requirements for Cryptographic Modules*)
  - Independent, private-sector, accredited testing laboratories with validation of test results by NIST and CSE (Canada)
- NIAP Common Criteria Evaluation and Validation Program
  - Testing commercial IT products against international standard (ISO/IEC 15408 *Common Criteria for IT Security Evaluation*)
  - Independent, private-sector, accredited testing laboratories with validation of test results by NIST and NSA

# A Comprehensive Approach

## Linking Critical Assessment Activities



# Key Milestones

- NIST Special Publication 800-37 (draft) released for public review

**28 October 2002**

**<http://csrc.nist.gov/sec-cert>**

- Public Comment Period

**28 October 2002 through 31 January 2003**

- Comments to NIST Computer Security Division

**[sec-cert@nist.gov](mailto:sec-cert@nist.gov)**

Note: NIST Special Publications 800-53 and 800-53A projected for completion and public review in Spring 2003

# Contact Information

100 Bureau Drive Mailstop 8930  
Gaithersburg, MD USA 20899-8930

## ***Program Manager***

Dr. Ron S. Ross  
(301) 975-5390  
[rross@nist.gov](mailto:rross@nist.gov)

## ***Special Publications***

Marianne Swanson  
(301) 975-3293  
[marianne.swanson@nist.gov](mailto:marianne.swanson@nist.gov)

## ***Gov't and Industry Outreach***

Dr. Stu Katzke  
(301) 975-4768  
[skatzke@nist.gov](mailto:skatzke@nist.gov)

## ***Assessment Scheme***

Arnold Johnson  
(301) 975-3247  
[arnold.johnson@nist.gov](mailto:arnold.johnson@nist.gov)

## ***Organization Accreditations***

Patricia Toth  
(301) 975-5140  
[patricia.toth@nist.gov](mailto:patricia.toth@nist.gov)

## ***Technical Advisor***

Gary Stoneburner  
(301) 975-5394  
[gary.stoneburner@nist.gov](mailto:gary.stoneburner@nist.gov)

**Comments to:** [sec-cert@nist.gov](mailto:sec-cert@nist.gov)

**World Wide Web:** <http://csrc.nist.gov/sec-cert>